VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Bezpečnosť bezdrôtových Wi-Fi sieti v podnikovom nasadení
Security of Enterprise Wireless Networks

2014 Marián Ďurkovič

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Marián Ďurkovič**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Bezpečnost bezdrátových WiFi sítí v podnikovém nasazení
Security of Enterprise Wireless Networks

Zásady pro vypracování:

Cílem práce je popsat problematiku bezpečnosti a zabezpečení bezdrátových sítí WiFi s následnou analýzou a úpravou existujícího zabezpečení v konkrétní podnikové sítí s ohledem na zvýšení bezpečnosti.
1. Úvod do problematiky zabezpečení WiFi sítí.
2. Popis současných bezpečnostních mechanismů a jejich známých zranitelných míst.
3. Provedení penetračních testů pomocí dostupných aplikací a srovnání proveditelnosti jednotlivých útoků (s přihlédnutím k současnému HW použitelnému pro brute-force útoky - paralelní systémy, FPGA, GPGPU).
4. Analýza zabezpečení podnikové síti založená na OSSTMM v.3.
5. Implementace úprav zabezpečení a přístupových mechanismů.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Milan Gudába**

Konzultant bakalářské práce: Mgr. Ing. Michal Krumnikl

Datum zadání: 16.11.2012

Datum odevzdání: 07.05.2014

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prehlásenie

Prehlasujem, že túto bakalársku prácu som vypracoval samostatne. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

V Ostravě 25. júla 2014 .....

Podpis študenta

Poďakovanie

Rád by som sa poďakoval všetkým, ktorí ma podporovali a bez ktorých by táto práca nikdy nevznikla. Hlavne p. Ing. Milanovi Gudábovi a p. Mgr. Ing. Michalovi Krumniklovi za odbornú pomoc, cenné rady a konzultácie ktoré mi poskytli pri vytváraní tejto práce.

Prehlásenie zástupcu spolupracujúcej právnickej alebo fyzickej osoby

„Súhlasím so zverejnením tejto bakalárskej práce podľa požiadaviek čl. 26, odst. 9 Študijného poriadku pre štúdium v bakalárskych/magisterských programoch VŠB-TU Ostrava."

V Bratislave 13. júna 2014

ERS systems spol. s r.o.
Šamorínska 10, 821 06 Bratislava
IČO: 36751995, DIČ: 2022356853
IČ DPH: SK2022356853
OR OS BA I, odd. Sro, vl.č. 45045/B

Podpis zástupcu

Abstrakt

Marián Ďurkovič: *Bezpečnosť bezdrôtových Wi-Fi sieti v podnikovom nasadení.* [Bakalárska práca]. Vysoká škola báňská – Technická univerzita Ostrava. Vedúci: Ing. Milan Gudába, konzultant: Mgr. Ing. Michal Krumnikl. Stupeň odbornej kvalifikácie: Bakalár v študijnom programe Informační a komunikační technológie. VŠB – TU v Ostrave 2014. 36 s.

Bakalárska práca sa venuje štandardom zabezpečenia bezdrôtových Wi-Fi sieti. Popisuje najčastejšie zraniteľnosti bezdrôtových sieti, či už v nesprávnych alebo zastaralých konfiguráciách. Hlavná časť bakalárskej práce sa venuje penetračným testom a pokusom o prienik do podnikovej siete s dostupným programovým vybavením a prostriedkami, s vysokým ohľadom na použitie moderných technológií paralelného výpočtu a porovnanie ich efektivity.

Kľúčové slová

Wi-Fi, bezpečnosť, penetrácia, bezdrôtové siete, IEEE 802.11, 802.1x, WEP, WPA, WPA2, RC4, TKIP, CCMP, EAP, PEAP

Abstract

Marián Ďurkovič: *Security of Enterprise Wireless Networks*. [Bachelor thesis]. VŠB-Technical University of Ostrava. Supervisor: Ing. Milan Gudába, consultant: Mgr. Ing. Michal Krumnikl. Academic qualification degree: Bachelor of Information and Communication Technology. VŠB – Technical University in Ostrava 2014. 36 s.

Bachelor thesis focuses on security of wireless Wi-Fi netvork´s standards. It describes the most common vulnerabilities of wireless networks based on wrong or outdated configurations. The main part of the thesis is dedicated to pen-tests and attempts to penetrate Enterprise network. Freely available software and utilities were used for this purpouse, focusing on modern technologies of parallel computing and compare effectivity.

Keywords

Wi-Fi, Security, Penetration, wireless networks, IEEE 802.11, 802.1x, WEP, WPA, WPA2, RC4, TKIP, CCMP, EAP, PEAP

Zoznam použitých symbolov, skratiek a termínov

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
CA	Certification Authority
CCMP	CTR with CBC-MAC Protocol
CPU	Central Processing Unit
CRC-32	Cyclic Redundancy Code
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
ICV	Integrity Check Value
IV	Initialization Vector,
KSA	Key Scheduling Alghorithm
MAC	Media Access Control
MIC	Message Integrity Check
MITM	Man-In-The-Middle
MSCHAPv2	Microsoft Challenge-Handshake Authentication Protocol version 2
PBKDF2	Password-Based Key Derivation Function 2
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwase Master Key
PRGA	Pseudo-Random Generation Algorithm
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QoS	Quality of Service
RSN	Robust Security Network
SSID	Service Set Identifier
STA	Station
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup

Obsah

1 Úvod do problematiky zabezpečenia Wi-Fi sietí....1
1.1 Vymedzenie problému a ciele práce....1
1.2 Problematika zabezpečenia Wi-Fi sietí....1
2 Popis súčasných bezpečnostných mechanizmov a ich známych zraniteľných miest....3
2.1 Štandard IEEE 802 11....3
2.2 Štandard IEEE 802.11b....3
2.3 Štandard IEEE 802 11a....4
2.4 Neskoršie doplnky štandardu IEEE 802.11....4
2.5 Pokrytie signálom a vzdialená správa AP....4
2.6 Autentizácia....5
2.7 SSID....5
2.8 MAC....6
2.9 WEP....6
2.9.1 Najčastejšie útoky na WEP šifrovanie....9
2.9.2 WEP Zhrnutie....10
2.10 WPA....10
2.10.1 Bezpečnosť WPA....11
2.11 WPA2....12
2.11.1 802.1x....12
2.11.2 WPA-PSK/WPA2-PSK....13
2.11.3 WPA-Enterprise/WPA2-Enterprise....13
2.11.4 Najčastejšie útoky na WPA/WPA2 šifrovanie....13
2.11.5 WPA/WPA2 Zhrnutie....17
2.12 WPS....17
2.13 Wordlist....18
2.14 Rainbow tabuľky....19
2.15 Hardvér CPU GPU FPGA a Cloud....19
3 Realizácia penetračných testov pomocou dostupných aplikácií a porovnanie realizovateľnosti (uskutočniteľnosti) jednotlivých útokov....22
3.1 Zadanie....22
3.2 Základné informácie o firme zadávateľa....22
3.3 Softvérové vybavenie....23
3.4 Prístupové body....23
3.5 Príprava....24
3.6 Slovníky....24
3.6.1 Postup....24

4 Analýza zabezpečenia podnikovej siete založená na OSSTMMv3....26
4.1 Wardriving....26
4.1.1 DoS Attack....27
4.1.2 Beck Tews Attack....27
4.1.3 Wordlist Attack....27
4.2 Prístupový bod ERS....29
4.3 Prístupový bod ERS office service....30
4.4 Prístupový bod ERS Systems....30
4.5 Prístupový bod ERS Holding....31
5 Implementácia úprav zabezpečenia a prístupových mechanizmov....32
5.1 Navrhované doplnkové nekomerčné riešenie....32
5.2 Navrhované doplnkové komerčné riešenie....33
6 Záver....34
Použitá literatúra....35

Zoznam ilustrácií

Obrázok 1: Schéma šifrovania typu WEP. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 128.).....8
Obrázok 2: Schéma dešifrovania typu WEP. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 129.).....8
Obrázok 3: 4-way handshake. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 137.).....15
Obrázok 4: Porovnanie výkonu CPU vs. GPU. (Zdroj: Wi-Fi Security: Cracking WPA With CPUs, GPUs, And The Cloud. [on-line]. [Citované 2014-03-14]. Dostupné na: http://www.tomshardware.com/reviews/wireless-security-hack,2981-8.html.....20

1 Úvod do problematiky zabezpečenia Wi-Fi sietí

Ľudia sa pohybujú, klasické drôtové siete zostávajú nehybne na mieste [1]. Možno práve to je dôvod prečo sú dnes bezdrôtové Wi-Fi siete také obľúbené. Bežní používatelia týchto sieti, ktorí ich využívajú všade kde je k tomu príležitosť (v práci, doma alebo sa len pripájajú sa na rôzne nezabezpečené AP), ani len netušia a nemajú odkiaľ vedieť, aké riziká sú spojené so stratou dôverných informácií spojených s využívaním týchto sietí. Vzhľadom k rôznym informáciám ktoré sa k nám dostávajú v poslednej dobe, ako napríklad zber informácií z nezabezpečených Wi-Fi sieti pomocou Google Street view áut či masívne odpočúvanie tajnými službami, je dôležité sa venovať zabezpečeniu všeobecne, nielen zabezpečeniu Wi-Fi sietí ale aj zabezpečeniu prístupových bodov jednotlivých používateľov. Digitálne súkromie máme len jedno, preto stojí za to si ho chrániť. Tak ako všade by malo platiť pravidlo, že cena zabezpečenia bezdrôtovej siete by nemala prekročiť cenu informácií alebo dát ktoré sú prenášané po tejto sieti.

1.1 Vymedzenie problému a ciele práce

Cieľom práce je uviesť čitateľa do problematiky zabezpečenia bezdrôtových Wi-Fi sietí, popísať najčastejšie spôsoby šifrovania využívaných na zabezpečenie týchto sietí a ich slabých miest. V súčasnosti sa totiž môžeme často stretnúť so zastaralými alebo žiadnymi spôsobmi šifrovania. V praktickej časti popíšem priebeh penetračných testov, realizovaných podľa OSSTMMv3 s použitím voľne dostupných nástrojov kladúc vysoký dôraz na použitie moderných trendov paralelného výpočtu pri dešifrovaní zabezpečenia, s následným návrhom zlepšení aplikovaných na existujúcu infraštruktúru s cieľom zvýšenia zabezpečenia bezdrôtovej Wi-Fi siete pre udržanie rastúcich požiadaviek bezpečnosti.

1.2 Problematika zabezpečenia Wi-Fi sietí

Najväčším problémom zabezpečenia nielen bezdrôtových Wi-Fi sietí je z mojich skúseností práve ľudský faktor. Tento problém by mala minimalizovať bezpečnostná politika

zabezpečenia spoločnosti, ktorá by mala zahŕňať školenia o povedomí informačnej bezpečnosti. Ide o spísané pravidlá, ktoré by sa mali dodržiavať pre zabezpečenie optimálnej bezpečnosti. Bežní používatelia technológií však nevedia, aké je dôležité dodržiavanie týchto pravidiel a keďže sú to pravidlá, ktoré ich v určitom zmysle obmedzujú, snažia sa ich obchádzať.

Druhým najčastejším problémom je takzvaný Rouge AP. Nemusí to nutne znamenať automatický pokus o prienik do siete, ale len spôsob, ako sa nepoučení zamestnanci môžu pokúšať pripojiť svoje zariadenia na internet a nechtiac vytvárajú bezpečnostné riziko. Názor: „My nemáme žiadny AP, naša politika neumožňuje mať vo firme bezdrôtový AP," jednoducho nemôže obstáť, nakoľko softvérový AP dokáže vytvoriť aj počítač pripojený do zabezpečenej siete.

Častým problémom býva aj zle nakonfigurované zariadenie s vysokou pravdepodobnosťou toho, že konfiguráciám sa nevenuje dostatočná pozornosť alebo konfiguráciu vykonáva niekto, kto sa dostatočne neorientuje v danej problematike a tým môže dôjsť k nesprávnej konfigurácií prístupového bodu a následne k bezpečnostnému riziku.

Je vhodné si uvedomiť, že bezpečnosti bezdrôtových sietí je potrebné venovať vyššiu pozornosť ako bezpečnosti klasickej drôtovej siete, už len z toho dôvodu, že komunikáciu môže útočník odchytiť oveľa jednoduchšie ako v prípade drôtovej siete. Toto môže byť veľký problém pokiaľ útočník používa anténu s vysokým ziskom, alebo špeciálnu smerovú, takzvanú „Yagi" anténu. V prípade cieleného útoku treba predpokladať, že útočník je dostatočne technicky zdatný a vybavený na takýto útok. Preto je potrebné zabezpečiť kontinuálne zvyšovanie zabezpečovania siete.

2 Popis súčasných bezpečnostných mechanizmov a ich známych zraniteľných miest.

2.1 Štandard IEEE 802 11

Dôvodom vzniku štandardu 802 11 bola potreba zaistiť jednotný štandard, pomocou ktorého mali pôvodne komunikovať mobilné zariadenia ako PDA a notebooky. Pred vznikom štandardu 802 11 bolo totiž nutné pre bezdrôtovú komunikáciu použiť produkty jedného výrobcu kvôli neexistencií jednotného štandardu a vzájomnej nekompatibilite [2].

Prvá verzia IEEE 802 11 štandardu bola vydaná v roku 1997. Definovala prenosové rýchlosti 1-2 Mbit/s. Norma pracuje v bezlicenčnom 2,4GHz rádiovom pásme a pokrýva prvé dve vrstvy modelu ISO/OSI. Štandard bol navrhnutý ako variant lokálnych sietí LAN založených na Ethernet (IEEE 802.3) [3].

2.2 Štandard IEEE 802.11b

V roku 1999 bolo vytvorené rozšírenie štandardu 802.11 na verziu 802.11b ktorého rýchlosti dosahovali 5,5 a 11 Mbit/s. V prípade nepriaznivých podmienok dokáže zariadenie na základe dynamickej zmeny prenosovej rýchlosti znížiť svoju prenosovú rýchlosť na 5,5 Mbit/s až základných 1-2 Mbit/s definovaných v pôvodnom 802.11 štandarde. Naopak v prípade zlepšenia podmienok prenosu dokáže zariadenie zvýšiť svoju prenosovú rýchlosť až na 11 Mbit/s. Štandard pracuje v bezlicenčnom pásme 2,4 GHz (2,4000 – 2,4835 GHz), v ktorom je možné súčasne využiť len 3 neprekrývajúce sa kanály. Pásmo 2,4 GHz nepatrí k najspoľahlivejším. Pracuje v ňom mnoho iných zariadení a prenos môže rušiť veľa iných zariadení ako napríklad Bluetooth alebo kurióznom prípade aj mikrovlna rúra [3].

2.3 Štandard IEEE 802 11a

V roku 1999 bolo vytvorené rozšírenie štandardu 802.11 o verziu 802.11a. Je definovaná pre bezlicenčné pásmo 5GHz, jeho maximálna teoretická prenosová rýchlosť je 54Mbit/s, ale reálne dosiahnuteľná rýchlosť sa pohybuje okolo 30 Mbit/s. Jeho výhodou je práve použitie menej využívaného 5GHz pásma, avšak nevýhodou je nemožnosť komunikovať so zariadeniami využívajúce štandard 802.11b a jeho ďalších doplnkov [3].

2.4 Neskoršie doplnky štandardu IEEE 802.11

IEEE 802.11 obsahuje množstvo ďalších doplnkov z ktorých sú najznámejšie a, b, g (zvýšenie prenosovej rýchlosti na 54Mbit/s) a n (vyššia priepustnosť pomocou MIMO antén). Najnovšími prírastkami v rodine 802.11 je zmena a doplnenie 802.11ac. V momentálnej revízií síce umožňuje dosahovať teoretické rýchlosti v maximálnej konfigurácií do 7 Gbit/s, avšak je vysoko energeticky náročný a maximálnu rýchlosť doplnku 802 11ac je možné v aktuálnej verzií využiť len do vzdialenosti 6 metrov od vysielača [4].

Nakoľko sú štandardy 802.11 definované veľmi benevolentne, vznikla krátko po vydaní prvého štandardu certifikačná autorita WECA (Wireless Ethernet Compatibility Alliance), ktorá testovala interoperatibilitu bezdrôtových zariadení rôznych výrobcov medzi sebou. Certifikačná autorita WECA bola v roku 2003 premenovaná na Wi-Fi alianciu [5].

2.5 Pokrytie signálom a vzdialená správa AP

Signál bezdrôtových sieti často zasahuje aj do nežiadúcich miest a presahuje i mimo budov. Na zabezpečenie takýchto miest existuje niekoľko spôsobov. Napríklad zníženie vyžarovacieho výkonu AP alebo nastavenie DHCP servera, pre prideľovanie IP adresy len známym MAC adresám.

Je dôležité nastaviť AP tak, aby nebola možná vzdialená správa ani správa cez bezdrôtové pripojenie. Ideálny stav je nastaviť konfiguráciu len pomocou drôtovej siete, pretože po získaní prístupu do siete by mohol útočník získať všetky potrebné informácie a na

ich základe zmeniť nastavenia siete. Rovnako dôležitá je fyzická bezpečnosť a umiestnenie AP tak, aby bol chránený pred možnosťou vykonať Reset zariadenia. Taktiež rozumným riešením je vytvorenie Virtuálnych LAN sieti s nastavením užívateľských skupín pre zabezpečenie prístupu k sieti.

2.6 Autentizácia

Ide o proces overenia identity používateľa. Na základe probe-request od klienta odpovie AP probe-response rámcom. Autentizácia predstavuje jednosmerné overenie identity klienta voči sieti, avšak nevýhodou je, že sieť sa autentizovať nemusí. V tomto prípade hrozí nebezpečenstvo útoku typu MITM (Man In The Middle Attack).

2.7 SSID

Názov SSID je skrátené označenie pre Service Set IDentifier. ktorý zariadenia štandardne vysielajú každých pár sekúnd. Pre pripojenie k sieti je nutné poznať daný SSID a kľúč. Občas sa však môže vyskytnúť situácia, keď je zariadenie nakonfigurované tak, aby svoj identifikátor nevysielalo. Toto zabezpečenie je však absolútne nedostatočné a nie je možné sa naň spoliehať, pretože žiadnym spôsobom nešifruje dáta, ktoré sú prenášané vzduchom a je možné ich bez problémov odchytiť.

Útočník dokáže SSID odchytiť zo siete. Association request totiž obsahuje SSID siete a ten sa prenáša bez akéhokoľvek zabezpečenia, či už je prenos dát šifrovaný alebo nie. Možné je použiť dva útoky na jeho zistenie:

- Pasívny: Monitorovať prevádzku a čakať kým sa začne nejaká stanica asociovať.
- Aktívny: Zaslaním sfalšovaného deautentifikačného rámca jednej alebo všetkým pripojeným staniciam a nasledovne vyčkať na opätovnú asociáciu, ktorá prebehne do niekoľkých sekúnd.

SSID nebolo navrhnuté ako ochrana siete, preto o ňom týmto spôsobom nemôžme uvažovať. Je ho však možné použiť ako doplnkové zabezpečenie, ktoré síce sieť neochráni, no môže útočníka spomaliť [6].

2.8 MAC

Ďalším spôsobom zabezpečenia je obmedzenie založené na filtrácií MAC adries. Podstata spočíva v tom, že AP bude asociovať len povolené MAC adresy. Iné ako povolené adresy budú automaticky odmietnuté a AP s nimi odmietne komunikovať. MAC adresa je unikátny a nemenný identifikátor, no je ho možné softvérovo zmeniť. Monitorovaním v pasívnom móde je možné jednoduchým spôsobom zistiť povolené MAC adresy, ktoré je možné odchytiť a následne zneužiť [7].

Rovnako ako v prípade skrývania SSID identifikátora, aj filtrácia MAC adries je len doplnkový spôsob ochrany bezdrôtovej Wi-Fi siete. Prenášané dáta niesu totiž žiadnym spôsobom šifrované a útočník ich dokáže jednoduchým spôsobom odchytiť. Z uvedeného dôvodu nad ním nemôžme uvažovať ako nad ochranou, ale iba ako nad doplnkovou službou.

2.9 WEP

Wired Equivalent Privacy alebo WEP bola pôvodná šifrovacia metóda v 802.11 a mala poskytnúť užívateľom bezpečnosť porovnateľnú s drôtovými sieťami. Kvôli slabej kryptografii sa tak nestalo a dnes je toto šifrovanie plne prelomené a považované za nedostatočné. WEP používa prúdovú šifru RC4 na zabezpečenie obsahu ICV a kontrolný súčet CRC-32 pre zaručenie integrity. Protokol neobsahuje žiadny mechanizmus správy kľúčov. Kľúč je statický a obe strany používajú pre šifrovanie a dešifrovanie ten istý kľúč.

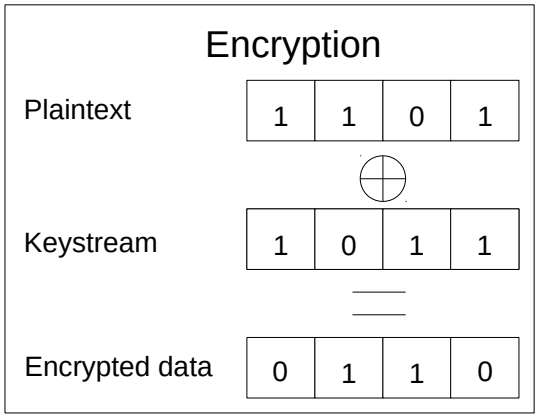
Zaužívané tvrdenie o pravidelnej a častej zmene prístupových hesiel v tomto prípade stráca relevanciu, nakoľko WEP šifrovanie je možné zlomiť do niekoľkých minút. Prakticky by bolo nutné meniť heslo každých 5 – 10 minút pri 64/128 bitovom kľúči. V ideálnych podmienkach je možné WEP prelomiť už v čase pod 1 minútu [8].

WEP používa 24 bitový inicializačný vektor (IV). Keď bol štandard WEP vo fáze návrhu (draft), bola obmedzená dĺžka kľúča v dôsledku exportných obmedzení kryptografických technológií. V prípade 64 bit kľúča je použitých 24 bitov pre IV a tým sa znížila skutočná veľkosť kľúča na 40 bitov. Ako náhle boli obmedzenia odstránené, bolo možné implementovať 128 bitový WEP s rovnakým základom, použitie 24 bitov pre IV a 104 bitov pre kľúč [9]. To je dôvod, prečo je možné v rôznej literatúre naraziť na 40 bitový a 104

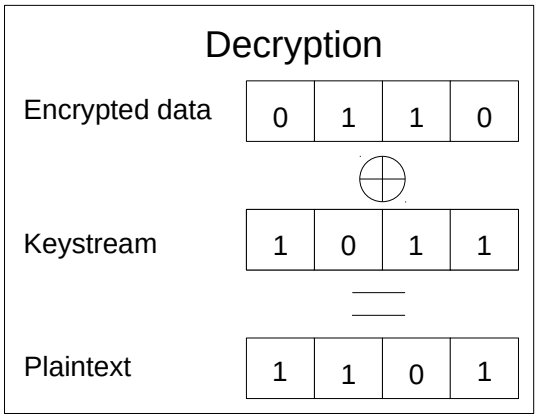
bitový kľúč, napriek tomu, že na inom mieste je označovaný ako 64 a 128 bitový.

Vzhľadom k malému keyspace “kľúčovému priestoru,” ktorý obsahuje približne 16 miliónov unikátnych IV, je možné IV znovu použiť.

Prúdovú šifru RC4 navrhol Ron Rivest pracujúci v RSA a práve táto šifra bola vybraná pre bezdrôtové šifrovanie a to pre svoju jednoduchosť a rýchlosť. RC4 je symetrická šifra čiže používa rovnaký kľúč pre šifrovanie a dešifrovanie dát. RC4 vytvára prúd bitov, ktoré sú XOR-ované s dátami ako je znázornené na obr. č. 1 a obr. č. 2. Pre dešifrovanie dát stačí jednoducho XOR-ovať šifrované dáta.



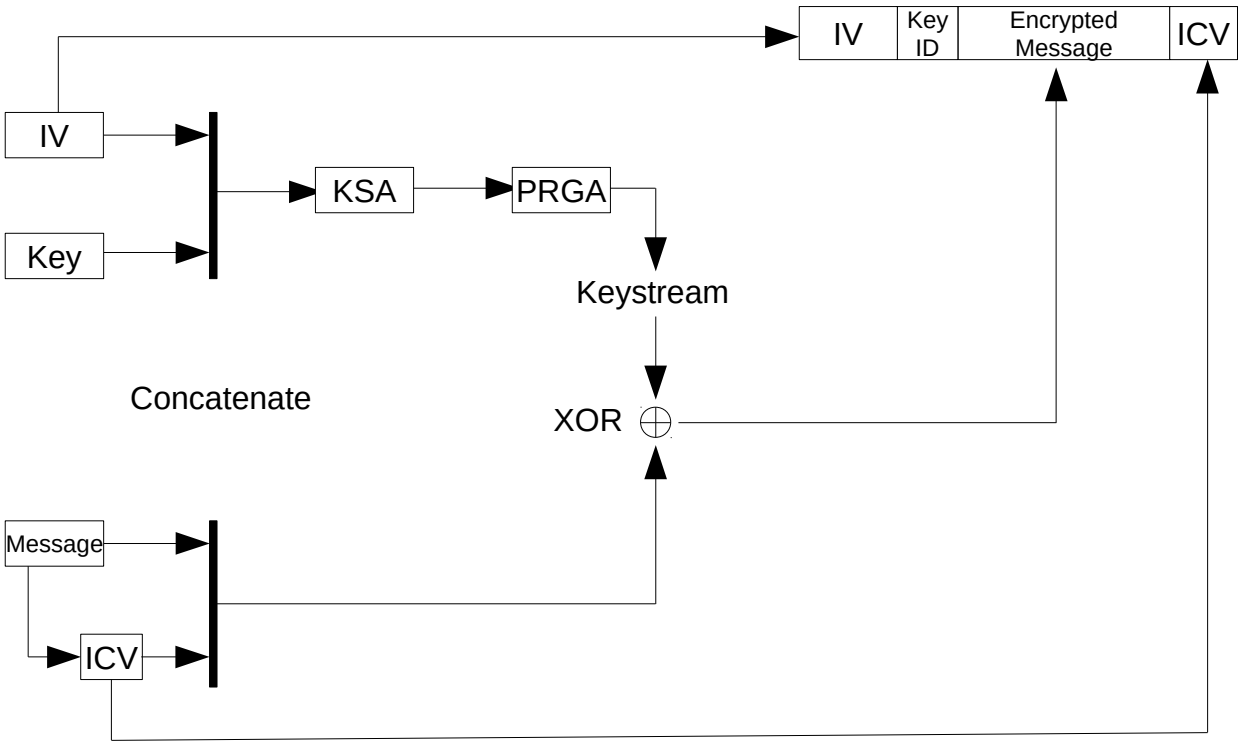
Obrázok 1: Ilustrácia šifrovania pomocou funkcie XOR. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 127.)



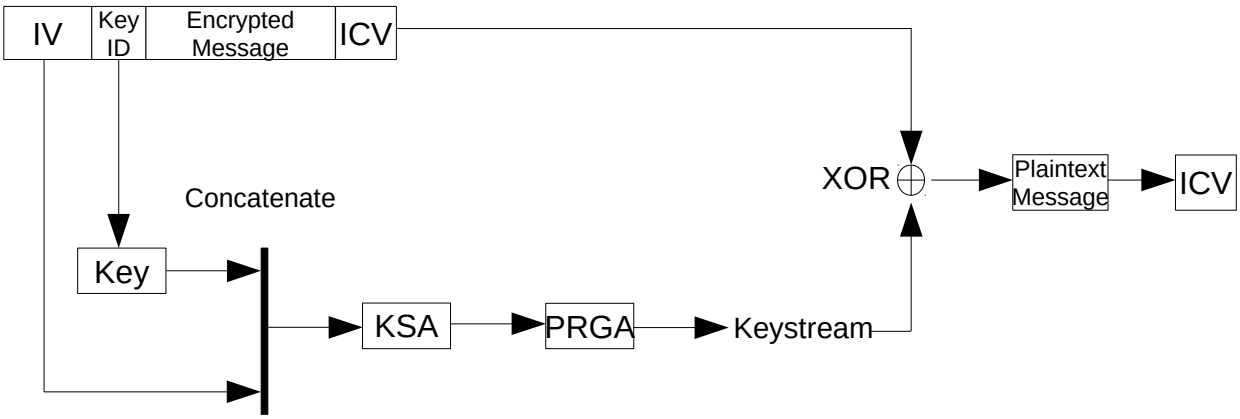
Obrázok 2: Ilustrácia dešifrovania pomocou funkcie XOR. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 127.)

RC4 sa skladá z 2 hlavných prvkov:

- KSA - Key Scheduling Alghorithm, ktorý inicializuje stav tabuľky s IV + WEP kľúč
- PRGA - Pseudo-Random Generation Algorithm, ktorý vytvára keystream.



Obrázok 1: Schéma šifrovania typu WEP. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 128.)



Obrázok 2: Schéma dešifrovania typu WEP. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 129.)

Nedostatky, ktoré sa stali základom známych útokov na WEP šifrovanie sú:

- použitie statického kľúča
- opakovanie IV
- rovnaký algoritmus na autentifikáciu a šifrovanie
- CRC-32 a operácie XOR
- šifrovanie ICV spolu s dátami
- prúdová šifra RC4

Väčšinu týchto problematických častí rieši šifrovanie známe ako WPA [9].

2.9.1 Najčastejšie útoky na WEP šifrovanie

Brute-Force Attack, taktiež známy ako útok hrubou silou, je výpočtovo veľmi náročný. Tento útok sa nevyužíva, nakoľko existuje množstvo ďalších a podstatne efektívnejších útokov.

Dictionary Attack (slovníkový útok). Jedná sa o vylepšenie Brute-Force útoku, kedy sa prehľadávanie hesla minimalizuje na slova z existujúceho slovníka.

FMS Attack, nazvaný podľa jeho tvorcov (S. Fluhrer, I. Martin, A. Shamir), ktorí poukázali na zraniteľnosť plánovania RC4 kľúčov. V prípade zachytenia 60 -100 paketov zašifrovaných pomocou takzvaných slabých IVS, je možné prelomiť zabezpečenie. Matematická zložitosť lámania hesla je v tomto prípade lineárna.

KoreK útok spočíva podobne ako FMS v linearite RC4 šifrovania a CRC súčtu (ICV). Umožňuje dešifrovať ktorýkoľvek zachytený rámec aktívnym iteratívnym spôsobom a tak získať jeho obsah.

PTW Attack, napriek tomu, že sa jedná o útok, ktorý využíva slabiny RC4 šifry, ide o úplne nový koncept. Nevyužíva zber slabých IVS, ale šifrované ARP pakety, z ktorých využíva len prvých 16 bajtov plaintextu, pri 104 bitovom WEP. Využíva skutočnosť, že niektoré polia v rámcoch sú známe. Tajný kľúč dokážeme zistiť na 50% z 40 000 a na 95% z 85 000 ARP rámcov [9].

Caffe-late Attack, jeho názov vychádza z času potrebného na prelomenie zabezpečenia typu WEP. V akejkoľvek kombinácii sa čas potrebný na prelomenie pohybuje do 6 minút. Caffe-late Attack je spôsob ako prelomiť šifrovanie bez nutnosti prístupu k AP. Využíva totiž klientsku stanicu, ktorá nemusí byť v dosahu AP. Na klientsku stanicu útočník zašle množstvo šifrovaných ARP žiadostí a z odpovedí klienta je možné vypočítať kľúč [10].

2.9.2 WEP Zhrnutie

Je vhodné si uvedomiť že šifrovanie Wi-Fi siete typu WEP bolo plne prelomené a získať prístup do siete je možný v priebehu pár minút. V praxi neexistuje účinný spôsob ako zabrániť prelomeniu tejto šifry. Jediným odporúčaním zostáva nutná výmena hardvéru, prípadne aktualizácia firmvér zariadenia pre podporu WPA.

2.10 WPA

Keď sa bavíme o prelomení Wi-Fi šifrovania, väčšina ľudí si myslí že ide len o šifrovanie typu WEP, čo nie je pravda. Rovnako zraniteľné je i šifrovanie typu WPA. Dokonca aj firemné siete ktoré sú zabezpečené pomocou protokolov EAP-TTLS či PEAP s dnes veľmi populárnou metódou MSCHAPv2 môžme považovať za nedostatočné chránené.

Kvôli problémom s WEP Wi-Fi Aliancia ratifikovala štandard známy pod názvom WPA (Wi-Fi Protected Access), ktorého výhodou bolo prijatie mechanizmov zo vznikajúceho tretieho návrhu 802.11i štandardu. Jedná sa o softvérové vylepšenie WEP s vysokým dôrazom na spätnú kompatibilitu s existujúcim hardvérom. Nakoľko ide len o vylepšenie pre softvér, nie je potrebné kupovať nové zariadene a postačuje upgrade firmvéru. Štandard WPA bol od začiatku chápaný len ako medzistupeň, ktorý mal vyriešiť problém s plne prelomeným zabezpečením typu WEP. Keďže išlo len o zaplátanie bezpečnostných problémov vo WEP s funkčnosťou na existujúcom hardvéri a kombináciou vznikajúceho štandardu 802.11i, vznikol nový štandard, ktorý však nie je kompatibilný ani s jedným z pôvodných štandardov.

Zásadnými rozdielmi oproti predchádzajúcemu štandardu sú použitie TKIP, vygenerovanie celkom nového šifrovacieho kľúča pre šifrovanie paketu, zdvojnásobenie

dĺžky IV a pre zaistenie integrity sa použije okrem CRC-32 aj kryptografický protokol MIC, ktorý je známy aj pod označením Michael.

TKIP (Temporal Key Integrity Protocol) je mechanizmus, ktorý využíva prúdovú šifru RC4 s kľúčom so štandardnej dĺžky 128 bitov. Bol navrhnutý tak, aby bol spätne kompatibilný s hardvérom vhodným pre WEP. Na rozdiel od WEP, ktorý používa statické kľúče, umožňuje použitie dynamických dočasných kľúčov, ktoré sa menia automaticky každých 10 000 paketov, a tým odstraňuje problém možnosti odvodenia kľúča.

MIC (Message Integrity Check), ktorý navrhol Neil Ferguson špeciálne pre WPA, je mechanizmus, ktorý zaisťujúci nelineárnu kontrolu integrity správ, čím zabraňuje zmene správ útočníkom a chráni pred použitím injekcie odchytenej komunikácie, takzvaným replay útokom.

802.11i predpokladá použitie zabezpečenia v rôznych prostrediach, ako sú podniky a v súčasne aj domácnosti. WPA preto obsahuje dva módy: WPA Enterprise a WPA-PSK [9].

2.10.1 Bezpečnosť WPA

Zabezpečenie WPA rieši mnoho nedostatkov, objavených v zabezpečení typu WEP. Avšak, ako som už spomenul, je potrebné ho chápať len ako medzistupeň v zabezpečení. WPA ako také bolo navrhnuté ako vylepšenie firmvéru pre starší hardvér, z čoho vyplývajú určité kompromisy ako napríklad použitie TKIP a RC4. Slabina tohto riešenia spočíva v tom, že v správnych podmienkach dokážeme dešifrovať šifrovaný obsah, no nedokážeme získať tajný kľúč. Momentálne je toto zabezpečenie v správnej konfigurácií dostačujúce a v najbližšej dobe sa nepredpokladá jeho prekonanie v zmysle získania tajného kľúča, no vo firemných sieťach sa odporúča použiť WPA2 [11].

WPA rieši nedostatky objavené vo WEP nasledujúcimi prvkami:

- Mixovanie kľúčov s každým paketom
- Sekvencovanie IV pre zabránenie replay-attack
- Nový algoritmus pre kontrolu integrity pomocou kryptografického MIC protokolu
- Mechanizmus distribúcie a výmeny kľúčov

2.11 WPA2

Zabezpečenie typu WPA2 je postavené už na dokončenom štandarde 802.11i. Alternatívne je označované ako RSN (Robust Security Network) a bolo ratifikované v júni 2004. Hlavnou výhodou je použitie AES-CCMP, ktorá nebola vo WPA použitá. Na jednej strane jednalo o nedokončený štandard, no na druhej strane je nutné poukázať aj na skutočnosť potreby hardvérovej akcelerácie z dôvodu vyššej hardvérovej náročnosti, ktorá vyplýva práve z použitia AES a tým nutného použitia nového hardvéru. Jednou z požiadaviek na WPA bola spätná kompatibilita s hardvérom bývalej generácie. Vo WPA2 je možné zvoliť TKIP, avšak už len ako voliteľný mechanizmus a primárne je použitie AES-CCMP povinné. Toto zabezpečenie je zamerané hlavne na autentizáciu protokolom 802.1x. Spätná kompatibilita nieje možná.

2.11.1 802.1x

Ide o riadenie prístupu k sieti. Riadený prístup k sieti je nutný v tom prípade, ak nemáme pod fyzickou kontrolou všetky pripojenia k sieti. Zabraňujeme tak neautorizovanému prístupu. V prípade bezdrôtového prístupu do siete je fyzické zabezpečenie vo väčšine prípadov nemožné. Riadenie prístupu zabezpečí prístup do siete len oprávneným osobám.

Štandard 802.1x bol pôvodne navrhnutý pre riadenie prístupu k drôtovým sieťam, no aplikuje sa aj v prípade bezdrôtových sietí. V prípade riadenia prístupu k bezdrôtovej sieti hrozí podstatne väčšie bezpečnostné riziko ako v prípade drôtových sietí. Pre drôtové siete je možné použiť aj iné techniky, ktoré v bezdrôtovom pripojení často vôbec neexistujú.

Riadenie prístupu k sieti je riešené na úrovni logických portov AP. 802.1x blokuje komunikáciu v sieti neoprávneným používateľom. Žiadateľovi sú najskôr blokované všetky prístupy okrem overenia u centrálneho autentizačného servera, takzvaný (uncontrolled) neriadený port. Po úspešnej autentizácií sa tento port prepne do režimu (controlled) Riadený port a sprístupní všetku komunikáciu [12].

2.11.2 WPA-PSK/WPA2-PSK

WPA-PSK (pre Shared Key) je mód zabezpečenia vhodný pre domácnosti a malé podniky. Autentifikácia zariadenia prebieha voči AP a nevyžaduje sa autentifikačný server. Klient však neautentifikuje prístupový bod. Každé zariadenie sa autentifikuje tým istým kľúčom, čo v prípade zmeny kľúča z akéhokoľvek dôvodu znamená nutnosť zmeny kľúča v každom zariadení. Dĺžka kľúča je obmedzená na minimálne 8 a maximálne 63 znakov [13].

2.11.3 WPA-Enterprise/WPA2-Enterprise

Ako nám napovedá názov, ide o nasadenie WPA v podnikových sieťach, Využíva sa najmä v podnikových sieťach, kde vyžadujeme prihlasovanie viacerých užívateľov s rôznymi prihlasovacími údajmi. Autorizáciu prenechávame centrálnemu RADIUS (Remote Authentication Dial In User Service) serveru namiesto AP. Výhodami použitia tohto riešenia je hlavne použitie centrálnej databázy používateľov, ich jednoduchá manažovateľnosť, šifrované overovanie a dôvernosť [14]. Autentifikácia je založená na EAP protokole a najčastejšie vykonaná prostredníctvom:

- EAP-TLS s klientskym a serverovým certifikátom
- PEAP hybridná autentifikácia, kedy je vyžadovaný certifikát iba na strane servera [9].

2.11.4 Najčastejšie útoky na WPA/WPA2 šifrovanie

Tak ako v prípade WEP, aj na šifrovanie WPA/WPA2 existuje niekoľko typov útokov. Samotné šifrovanie je však oveľa odolnejšie voči prelomeniu a útoky, ktoré bolo možné realizovať voči WEP tu väčšinou nemajú žiadny účinok.

Pasívny slovníkový útok patrí medzi prvé funkčné útoky na šifrovanie WPA/WPA2 – PSK, avšak nie je možné ho realizovať na EAP. Útočník čaká na asociáciu klienta a AP, ktorá

prebieha pomocou 4-way handshake paketov. Z nich je možné dešifrovať šifrovací kľúč na základe nešifrovaných náhodne generovaných čísel prenášaných v úvode komunikácie klienta a AP a slova zo slovníka. Hľadané heslo sa musí nachádzať v slovníku.

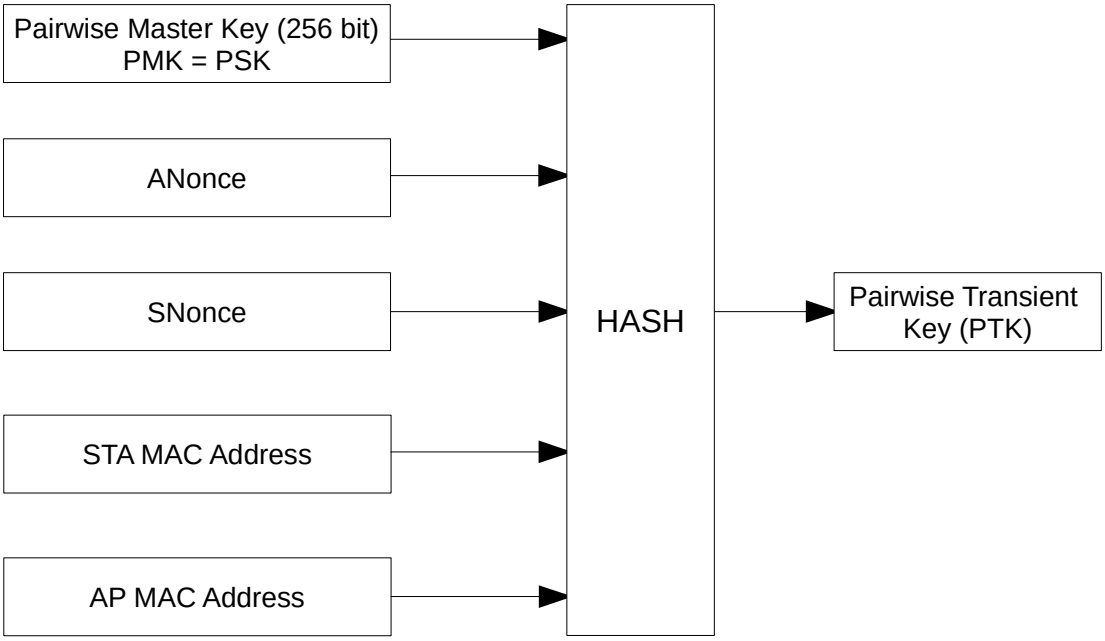
Aktívny slovníkový útok sa líši od predchádzajúceho iba v tom, že útočník nečaká na pripojenie klienta, ale existujúceho klienta odpojí od AP a klient sa následne snaží opätovne pripojiť, následkom čoho útočník odchytí 4-way handshake.

Honeypot je softvérový AP podstrčený útočníkom, ktorý sa tvári ako legitímny AP, no je ovládaný útočníkom. Na vytvorenie Honeypot AP stačí poznať ESSID, ktoré klientská stanica vysiela do éteru pri pokuse o nadviazanie spojenia, a typ šifrovania.

Na prelomenie 4-way handshake musí útočník poznať 4 parametre, z ktorých sa všetky prenášajú nešifrovane:

- Anonce - náhodne vygenerované číslo, ktoré posiela AP pri nadväzovaní spojenia s klientom
- Snonce - náhodne vygenerované číslo ktoré posiela klient pri nadväzovaní spojenia s AP
- MAC adresu AP
- MAC adresu klienta

Tieto informácie sa nachádzajú v 2 správach zo 4 správ a to buď v prvej a druhej, alebo tretej a štvrtej správe. Pri pokuse o pripojenie k Honeypot prebehnú len prvé dve správy a následne skončí handshake s chybou, nakoľko Honeypot nepozná PMK, no handshake je úspešne odchytený [9].



Obrázok 3: 4-way handshake. (Prevzaté z: AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009, str. 137.)

Beck-Tews je útok nazvaný podľa mien jeho tvorcov - Erik Tews a Martin Beck. Ide o útok na WPA-PSK s použitím TKIP, útok na WPA2 s CCMP nie je možné realizovať. Týmto typom útoku nie je možné odhaliť tajný kľúč, ale umožňuje dešifrovať obsah paketov. Slabým miestom je použitie TKIP, ktorý bol zvolený pre spätnú kompatibilitu s WEP, a preto si zachováva aj niektoré nedostatky práve z tohto typu zabezpečenia [15]. Pre Realizáciu tohto typu útoku je nevyhnutné, splniť niekoľko podmienok:

- Použitie dlhej doby rekeyingu (doby zmeny kľúčov) štandardne 3600 sekúnd.
- Zapnutá služba QoS (Quality of Service)
- IPv4 rozsah kde väčšina adresy je známa

Ohigashi-Morii je rozšírený útok založený na Beck-Tews útoku, za ktorým stoja Toshihiro Ohigashi a Masakatu Morii. Útok vylepšuje predchádzajúci Beck-Tews útok odstránením nutnosti použitia QoS na AP a pridáva do útoku MITM. Útok je možné realizovať voči hocijakému WPA-PSK AP avšak útok nefunguje na WPA2. Počas útoku dochádza k výpadku siete. Rovnako ako v predchádzajúcom prípade, týmto útokom nie je možné dešifrovať tajný kľúč, je však možné dešifrovať pakety, prípadne zasielať falošné správy smerom ku klientovi a AP [16].

Hole196 je slabina, ktorá sa nachádza v sieťach zabezpečených pomocou WPA/WPA2 a taktiež ako v PSK, tak aj v Enterprise režime. Útok je možné realizovať len z vnútra siete v prípade, ak poznáme tajný kľúč. Nejedná sa teda o útok na tajný kľúč a tajný kľúč nie je možné týmto spôsobom zistiť. Podstatou útoku je zmena ARP smerovacích tabuliek a možnosť odchytávať komunikáciu útočníkom. V prípade PSK tento útok nemá veľké opodstatnenie, nakoľko v prípade, že poznáme kľúč, dokážeme rovnako dešifrovať odchytenú komunikáciu bez nutnosti zmeny smerovacích tabuliek [17].

MITM útok je možné vykonať na PSK aj na Enterprise. Enterprise je však v tomto prípade zaujímavejší. Útok je možné využiť na získanie správ Challenge a Response v MS-CHAPv2, kedy útočník zachytáva všetky správy a posiela ich ďalej v tomto prípade v nezmenenej podobe. Útočník tak získa meno v nešifrovanej podobe a Hash hesla Challenge/Response správy, ktoré je možné dešifrovať slovníkovým, prípadne Brute-Force útokom.

PEAP, ako bolo popísané vyššie, vyžaduje certifikát iba na strane servera. To znamená, že nesprávne nakonfigurované zariadenie neoveruje certifikát servera a akceptuje ho tak ako je. Nastavenie overovania certifikátu je možné, ale keďže nie je povinne, môžeme takmer s istotou tvrdiť, že nebezpečná konfigurácia sa na sieti bude vyskytovať. Neoverenie certifikátu servera má za následok, že klient akceptuje akýkoľvek certifikát. Preto je možné vykonať útok typu MITM prípadne Rouge AP s Free Radius serverom pre odchytenie MSCHAPv2 správ Challenge a Response, čím útočník získa nešifrované prihlasovacie meno a Hash hesla ktorý je možné následne dešifrovať. Útočník tak získa prístup nielen do siete, ale často aj k službám Active-Directory, VPN, e-mail a podobne. PEAP napriek svojej známej zraniteľnosti sa vo veľkej miere používa z toho dôvodu, že je podporovaný v prevažnej väčšine systémov. Zároveň je to metóda zabezpečenia, ktorá sa veľmi jednoducho konfiguruje. Na rozdiel od EAP-TLS, ktorý túto chybu neobsahuje a je momentálne považovaný za najbezpečnejší. Okrem ťažšej konfigurácie vzniká problém aj s distribúciou certifikátov. Situáciu komplikuje aj fakt, že klientske stanice sú nakonfigurované aby dôverovali centrálnym certifikačným autoritám (CA) a ak útočník vlastní certifikát vydaný centrálnou autoritou, klientské stanice tento certifikát potichu akceptujú. Bezpečnejším riešením je použitie takzvaného Self-signed certifikátu aj za cenu zvýšenej náročnosti ich manažmentu [27].

2.11.5 WPA/WPA2 Zhrnutie

WPA/WPA2 neporovnateľne zvýšilo úroveň bezpečnosti bezdrôtových sieti oproti WEP, avšak existuje niekoľko praktických útokov na získanie tajného kľúča, a to ako v prípade PSK, tak aj v prípade Enterprise nastavenia. Niektoré útoky neumožňujú získanie tajného kľúča, ale sú zamerané na odhalenie šifrovanej komunikácie.

V prípade PSK sa odporúča používať WPA2 s CCMP a bezpečným prístupovým heslom a jeho pravidelná zmena. Ak sme však nútení použiť WPA s TKIP, odporúča sa znížiť čas rekeyingu na minimum.

V prípade použitia Enterprise nastavení je potrebné podotknúť, že PEAP a aj EAP-TLS je úplne bezpečné v prípade, že je bezpečne nakonfigurované. Avšak v prípade PEAP sa toto v bežnej prevádzke dá len veľmi ťažko zabezpečiť.

2.12 WPS

Wi-Fi Protected Setup je voliteľný štandard, ktorého úlohou je jednoduché a bezpečné nastavenie prístupu do zabezpečenej Wi-Fi siete a je možné sa s ním stretnúť iba pri PSK. WPS dokáže automaticky nakonfigurovať metódu šifrovania, metódu autentizácie a SSID bez akejkoľvek nutnosti zásahu používateľa. Štandard definuje niekoľko možností nastavenia konfigurácie, ktoré sú prenášané pomocou niekoľkých EAP správ. Pre získanie certifikácie WPS musia byť splnené len prvé dve metódy. Metóda formou PIN kódu a PCB.

- PIN je vo väčšine prípadov nalepený na štítku AP, avšak v nastaveniach je možné zmeniť časť tohto kódu. PIN má dĺžku 8 číselných znakov.
- PCB (Push Button Configuration) je kombinácia tlačidiel ktoré je potrebné stlačiť krátko po sebe. Po ich stlačení dochádza k prenosu nastavení a konfigurácie.
- NFC (Near Field Communication) obe zariadenia musia obsahovať NFC čip. K prenosu konfigurácie dochádza po vzájomnom priblížení zariadení. V praxi sa s touto implementáciou takmer nieje možné stretnúť.
- USB nastavenia sa prenášajú pomocou USB pamäťového zariadenia.

Pôvodná myšlienka WPS stavia na predpoklade, že útočník na uhádnutie hesla musí vyskúšať 10^8 (=100.000.000) kombinácií Brute-Force útokom. Stefan Viehböck, podľa ktorého dostal útok názov Viehböck attack, zistil, že posledné ôsme číslo kódu je iba kontrolný súčet, čo znamená zníženie počtu pokusov na 10^7 a dopočítanie posledného čísla kódu. Okrem toho implementácia WPS rozdeľuje týchto osem čísiel na dve polovice a potvrdzuje správnosť každej z nich. To znamená zníženie počtu pokusov na $10^4 + 10^4$ (=20.000) kombinácií. Ako už bolo spomenuté ôsme číslo je vždy kontrolný súčet, čo drasticky znížilo čas potrebný na prelomenie kódu Brute-Force útokom na $10^4 + 10^3$ (=11.000) kombinácií + dopočítanie kontrolného súčtu.

Pri niektorých zariadeniach WPS nie je možné vypnúť a WPS štandard neobsahuje implementáciu uzamknutia zariadenia proti Brute-Force útoku, no napriek tomu výrobcovia zariadení implementujú svoje vlastné riešenia, ktoré čiastočne zabraňujú Brute-Force útoku na WPS [18].

2.13 Wordlist

Brute-Force attack býva poslednou alternatívou útoku (nielen) na Wi-Fi sieť z dôvodu, že sa jedná o časovo a výpočtovo veľmi náročný proces. Zdroje potrebné pre Brute-Force útok rastú exponenciálne s dĺžkou kľúča. Algoritmus PBKDF2 sa používa na odvodenie PMK z tajného kľúča. Každé tajné heslo je 4096 krát Hašované pomocou SHA-1 a prvých 256 bitov na výstupe je porovnávaný Hash s vygenerovanou počiatočnou výmenou kľúčov. Toto je dôvod, prečo Wordlist attack nahrádza Brute-Force attack, ktorý je limitovaný počtom slov v slovníku. Nevýhodou slovníkového útoku je fakt, že dokážeme odhaliť len heslo, ktoré máme v slovníku. Naproti tomu pomocou Brute-Force sme teoreticky schopní odhaliť akokoľvek zložitý kľúč, avšak problémom je práve exponenciálna zložitosť [9]. Akokoľvek dobre nastavenú politiku hesiel si jej používatelia majú tendenciu zľahčovať, a to z rôznych dôvodov. Tým sa vystavujú potenciálnemu riziku. Použitie aspoň jedného veľkého písmena a čísla sa najčastejšie obchádza tým, že prvý znak hesla je veľké písmeno, a posledným znakom je číslo väčšinou číslo 1. Rovnako dĺžka hesla býva najčastejšie 8 znakov, čo je pri WPA-PSK/WPA2-PSK jeho minimálna dĺžka. Komplexnejším spôsobom generovania hesla je substitúcia podobných znakov, kedy sa znak „o“ nahradí číslom „0“ a podobne. Tieto všetky kombinácie a substitúcie kvalitný slovník obsahuje.

2.14 Rainbow tabuľky

Rainbow tabuľky sú predvypočítané tabuľky pre reverznú kryptografickú Hash funkciu, ktoré zvyčajne využívame na prelomenie Hashu hesla, v tomto prípade WPA-PSK tajného kľúča. V prípade WPA-PSK nie je rainbow tabuľka nič iné ako wordlist, ktorý je už vopred vypočítaný na porovnanie Hashu hesla. Vytvoriť takúto tabuľku je rovnako náročné, ako priamy výpočet tajného hesla pri súčasnom porovnávaní Hashu. Jeho výhodou je však práve to, že výpočet nie je nutné opakovať pri každom pokuse o zistenie tajného hesla, ale jednoduchým porovnaním, ktoré už ale nie je náročné, ako samotný výpočet. Pre porovnanie počítač Pentium 3 dokáže otestovať priamym výpočtom 12 hesiel za sekundu a tento istý počítač dokáže otestovať 18 000 hesiel za sekundu pomocou rainbow tabuľky. Toto riešenie však má aj niekoľko nevýhod. Rovnako ako v prípade slovníku sa heslo musí nachádzať vo vopred vypočítanej forme v tabuľke, inak bude výsledok hľadania vždy negatívny. Okrem toho pre výpočet Hash sa používa názov SSID a jeho dĺžka. To znamená že Hash pre AP s názvom Linksys bude vždy iný ako pre AP s názvom D-Link pri súčasne rovnakom hesle to je dôvod, prečo nie je možné vytvoriť univerzálne tabuľky pre hľadanie hesla na ľubovoľnom AP [19].

2.15 Hardvér CPU GPU FPGA a Cloud

WPA a aj WPA2 využíva Funkciu PBKDF2 definovanú v RFC2898. Funkcia PBKDF2 je iterovaná 4096 krát a jej výstupom je 256 bitový SHA-1 kľúč. 4096 iterácií je veľmi dôležité číslo, ktoré sa postupne s narastajúcim výkonom môže stať úzkym hrdlom celého zabezpečenia [27].

Praktický útok na získanie tajného kľúča WPA/WPA2 pomocou slovníkového útoku preto predstavuje 4096 potrebných iterácií každého hesla ktorých v slovníku môžu byť milióny. S dobre optimalizovaným slovníkom máme väčšiu šancu na odhalenie tajného kľúča ako s neoptimalizovaným slovníkom, preto je rozumné zamyslieť sa nad výberom zdrojov pre vytvorenie vlastného slovníka popísaného v kapitole 3.6.. 4096 iterácií každého hesla so sebou prináša nutnosť disponovať dostatočným výpočtovým výkonom.

CPU. Všetky nástroje spomenuté v kapitole 4.1.3 podporujú lámanie hesla pomocou CPU. Líšia sa však podporovanými inštrukčnými sadami zrýchľujúcimi výpočet alebo priamo

zameraním daného softvéru. Lámanie hesla je proces ktorý je možné veľmi efektívne paralelizovať. Počítač použitý na testy mal výpočtový výkon CPU na úrovni približne 4000 PMK/s.

GPU. Lámanie hesiel za pomoci GPU/GPGPU rovnako, ako bolo spomenuté vyššie v prípade CPU je možné veľmi efektívne paralelizovať a túto paralelizáciu je možné s nástupom technológií ako OpenCL a Nvidia CUDA veľmi dobre prevádzkovať na podporovaných grafických kartách. Nevýhodou v tomto prípade je podstatné zvýšenie spotreby elektrickej energie ktoré však kompenzuje niekoľkonásobný výkon pri porovnaní s výpočtovým výkonom CPU. Pomocou grafickej karty použitej v testoch bol výpočtový výkon jednej karty na úrovni 21000 PMK/s.

	Intel Core i5-2500K	Nvidia GeForce GTX 460 1 GB
Cores	4 (no HT)	336
Clock Speed	3.3 GHz (base)	1350 MHz
Wireless Security Auditor	4752 passwords/s	18 105 passwords/s
Pyrit Benchmark	3949.13 PMKs/s	17 771.6 PMKs/s
Pyrit w/CoWPAtty	3306.85 passwords/s	19 077.15 passwords/s
Time To Crack Passwords Between 1 and 6 Characters (Alphanumeric)	140 days, 14 hours (WSA)	35 days (Pyrit)
Time To Crack Passwords Between 1 and 8 Characters (Alphanumeric)	1480 years, 311 days (WSA)	368 years, 319 days (Pyrit)

Obrázok 4: Porovnanie výkonu CPU vs. GPU.
(Zdroj: Wi-Fi Security: Cracking WPA With CPUs, GPUs, And The Cloud. [on-line]. [Citované 2014-03-14]. Dostupné na: http://www.tomshardware.com/reviews/wireless-security-hack,2981-8.html

FPGA. Field-Programmable Gate Array, je typ čipu, ktorý je možné naprogramovať až po výrobe na vykonávanie ľubovoľnej operácie a nie je obmedzený výrobcom na vykonávanie určitého typu inštrukcií, ako je to v prípade CPU. Najznámejším výrobcom FPGA ktoré sú implicitne podporované množstvom softvéru na lámanie hesiel, sú produkty spoločnosti Pico Computing. Napriek tomu, že FPGA od Pico Computing obsahujú pamäte typu RAM, na základe diskusie s tvorcom aplikácie, Davidom Hultonom vyplýva, že algoritmus využíva iba internú cache, tzv. BlockRAM. Pamäť RAM má tendenciu byť

pomalšia a vzniká problém s paralelným prístupom k tomuto typu pamäte v čase, keď sa snažíme vytvoriť viacero inštancií SHA-1 jadier. Nemožno preto očakávať výhodu alebo zvýšenie výkonu s použitím pamäte typu RAM. Teoreticky by sme teda mohli uvažovať, ak teda nepotrebujeme pamäť typu RAM, že by sme implementovali algoritmus pre FPGA ktoré sa typicky používali na ťažbu digitálnej meny Bitcoin, a to hlavne z dôvodu cenovej dostupnosti. Ako referenčný model berieme jedno z FPGA, ktoré sú typicky osadené čipom Xillinx Spartan-6 s frekvenciou 200MHz (pre jednu iteráciu SHA-1 jadra). Ak teda vezmeme do úvahy počet potrebných iterácií PBKDF2 funkcie, dostaneme sa na odhadovanú hodnotu 5 - 20 000 Hash/s. na jednom jadre. Následnou paralelizáciou jadier je možné výkon zvýšiť n-krát v závislosti od počtu paralelných inštancií SHA-1 jadier, ktoré dokážeme vtesnať na čip. Problém však môže spôsobiť aj komunikačné USB rozhranie v závislosti od toho, aké rýchle môžu byť naše jadrá. Túto implementáciu je teoreticky možné vytvoriť na ľubovoľnom FPGA. Výhodou oproti GPU je pri porovnateľnom výkone podstatne nižšia spotreba elektrickej energie alebo naopak, neporovnateľne vyšší výkon pri rovnakej spotrebe elektrickej energie. V Súčasnosti môžeme za najvýkonnejší FPGA čip považovať Kintex-7, avšak náklady hovoria skôr v prospech lacných Spartan-6 čipov.

Cloud. Spomedzi týchto riešení sú najznámejšie a najpoužívanejšie dve služby. Ich výhodou je nulová obstarávacia cena a náklady spojené len s prevádzkou:

- CloudCracker – slovníky sú pevne dané a upravené prevádzkovateľmi serveru. Nevýhodou je práve použitie anglických slovníkov, no na druhú stranu služba garantuje 100% prelomenie zabezpečenia MSCHAPv2 používaného v zabezpečení typu WPA/WPA2 Enterprise, ktoré je encapsulované v PEAP viď. kapitola 2.11.4. Rýchlosť lámania hesla je 300 mil. hesiel za 20 minút, čo predstavuje 250 000 PMK/s [28].
- Amazon EC2 – na rozdiel od služby CloudCracker nedefinuje žiadne slovníky a takisto hardvér je možné škálovať. Toto riešenie je vhodné na vystavanie vlastného riešenia.

3 Realizácia penetračných testov pomocou dostupných aplikácií a porovnanie realizovateľnosti (uskutočniteľnosti) jednotlivých útokov

Podrobné informácie o heslách, konkrétnych konfiguráciách či podrobnom programovom vybavení a nastaveniach nebudú v tejto práci zverejnené z dôvodu zabezpečenia bezpečnosti firmy. Všetky zverejnené nastavenia a materiály sa budú vzťahovať na pôvodné nastavenia, ktoré boli upravené.

3.1 Zadanie

Penetračné testy budú vyhotovené a orientované na zabezpečenie Wi-Fi prístupových bodov. V prípade úspešného prelomenia zabezpečenia nie je povolené ďalej skenovať a prehľadávať sieť a odchytávať komunikáciu. Testy prebehnú na základe metodickej príručky OSSMTv3 formou White-Box testovania. To znamená, že zadávateľ oboznámil testujúcu osobu so stavom siete a zabezpečením.

3.2 Základné informácie o firme zadávateľa

Zadávateľská firma ERS systems spol. s r.o. zadala požiadavku na vykonanie analýzy zabezpečenia bezdrôtových prístupových bodov administratívnej budovy sídla svojej materskej firmy ERS Holding spol. s r.o.

ERS Holding sa primárne sústreďuje na oblasť stavebníctva a nehnuteľností, prenájom zasadacích priestorov, účtovníctvo a daňové poradenstvo. V budove sa nachádzajú výlučne kancelárske priestory spoločnosti.

Názov spoločnosti:	ERS Holding spol. s r. o.,
Ulica:	Šamorínska 10
Mesto:	Bratislava
PSČ:	821 06

3.3 Softvérové vybavenie

Operačným systémom na pracovných staniciach je Microsoft Windows vo verziách od XP až Windows 7 s pripojením na Active-Directory doménu. Na serveroch beží serverová verzia Windows 2008 R2. Poštový server beží na distribúcií CentOS linux 5.5.

3.4 Prístupové body

V budove spoločnosti ERS Holding sa nachádzajú tri prístupové body, ktorých zabezpečenie sa postupne pokúsime prekonať. Nebezpečenstvo zle nakonfigurovaného prístupového bodu je veľkým bezpečnostným rizikom, pretože z vlastnej skúsenosti viem, že bezdrôtové prístupové body sa často nachádzajú vo vnútornej sieti spoločnosti a teda nie je potrebné prekonávať iné zabezpečenia.

Prístupové body sú určené zamestnancom spoločnosti pre prácu z prenosných zariadení, ako notebooky PDA alebo smartfóny.

3.5 Príprava

Vybavenie, pomocou ktorého budú vykonávané testy:

- Notebook s virtualizovaným Kali linux 32bit
- USB Wi-Fi adaptér Alfa AWUS036H (Realtek 8187)
- USB Wi-Fi adaptér NoName (Realtek 8187)
- Anténa všesmerová 5dBi 2,4 GHz RP-SMA
- Anténa smerová 7dBi 2,4 GHz RP-SMA
- Desktop PC Intel i7 2550, Nvidia 480 GTX, 16GB RAM (CPU/GPU Crack)
- Smartphone s OS Android (Wardriving)

3.6 Slovníky

Z časových dôvodov nebudú vykonávané Brute-Force útoky. Kvalitný slovník obsahuje aj samotný Kali linux. Jeho nevýhodou je však to, že sa jedná o anglický slovník a teda v našom regióne nie veľmi vhodný, preto som sa rozhodol vytvoriť vlastný slovník. Naskytá sa niekoľko možností, ako napríklad softvér John the Ripper, Crunch, či využitie už pred pripraveného slovníka [26].

3.6.1 Postup

Ako základ slovníka použijeme Aspell checker:

```
1. # aspell -l sk dump master > SK.dic
2. # cstocs iso-8859-2 ascii SK.dic > SK.ascii
3. # sed 's/\//\n\//' SK.ascii | grep -v '^/' > SK.final
```

Doplníme ďalšie slová z vhodných stránok:

```
1. # mkdir /adresar
2. # cd /adresar
3. # wget -r http://nejakastranka.sk
4. # perl wyd.pl -n -o - hesla.txt -/adresar
```

Ak predpokladáme, že heslo môže byť iba číselná kombinácia, použijeme nástroj Crunch [26].

```
1. # crunch 8 64 0123456789 > cisla.dic
```

Takto pripravený slovník je vhodný na prelomenie jednoduchých hesiel, avšak heslá s pridanými znakmi, alebo substitúciami neobsahuje. Preto využijeme skript Giga Wordlist Creator, pomocou ktorého spojíme všetky slovníky, a pomocou John The Ripper vytvoríme 50 kombinácií z každého slova, prípadne môžeme skript editovať podľa vlastnej potreby, takže dokážeme odhaliť aj heslá ako 1heslo, heslo1, Heslo1 a podobne. Optimalizujeme dĺžku hesiel na 8 – 63 znakov, odstránime duplicity a zoradíme podľa abecedy. Tieto operácie je možné vykonať aj manuálne, avšak Giga Wordlist Creator nám uľahčí prácu [20].

4 Analýza zabezpečenia podnikovej siete založená na OSSTMMv3

OSSTMMv3 - Open Source Security Testing Methodology Manual je Open-Source verejne dostupná metodická príručka zameraná na testovanie bezpečnosti a zvýšenie kvality podnikovej bezpečnosti a taktiež udáva metodiku a stratégiu pre testovanie. OSSTMM predpokladá Black-Box testing a využíva premyslenú skladbu používaných testov ktoré sú konzistentné a kedykoľvek opakovateľné pre porovnanie progresu v zabezpečení. V našom teste nebudeme testovať všetky body, ale len vybrané kapitoly, ktoré boli dohodnuté s vedením spoločnosti. Vzhľadom na rozsah a zameranie práce budú testy špecifikované v obmedzenej podobe.

4.1 Wardriving

Wardriving je metóda vyhľadávania bezdrôtových sieti Wi-Fi osobou jazdiacou autom pomocou počítača, no v posledej dobe hlavne pomocou smartfónov. V tomto prípade sme vykonali Wardriving pomocou smartfónu so systémom Google Android so zapnutým GPS modulom a aplikáciou Wigle Wifi Wardriving [7].

Pomocou tejto aplikácie sa nám podarilo zistiť prítomnosť 4 AP v budove čo je rozdiel oproti pôvodnému číslu, ktoré sme dostali od zadávateľa. Skenovaním sme zistili nasledovné nastavenia:

```
1. # ERS Holding          xx:xx:xx:xx:xx:xx   WPA2 WPS
2. # ERS Systems          xx:xx:xx:xx:xx:xx   WPA/WPA2
3. # ERS office service   xx:xx:xx:xx:xx:xx   WPA-PSK-TKIP
4. # ERS                  xx:xx:xx:xx:xx:xx   WEP
```

Z názvov je jednoznačné, že všetky prístupové body patria zadávateľovi.

4.1.1 DoS Attack

Je možné realizovať viacerými spôsobmi. Najjednoduchším spôsobom je útok proti jednému zariadeniu s použitím prepínača -c, alebo proti všetkým zariadeniam pripojeným na AP bez použitia prepínača.

```
1. # airodump-ng -1 100 -a aa:bb:cc:dd:ee:ff mon0
```

Pri použití tohto útoku je možné realizovať útok pomocou Rouge AP a tak odchytávať inicializačnú komunikáciu v PSK alebo EAP, napríklad PEAP a 802.1x autentizáciou.

4.1.2 Beck Tews Attack

Pôvodnou úlohou Beck Tews útoku injekcia ARP paketov a tým možnosť spôsobiť ARP poisoning. Tento útok je obmedzený na 7 paketov na približne 12 minút. Rozšírením je potom možnosť DHCP ACK DNS útoku. Pre názornosť vykonáme iba útok na získanie reverzného MIC kľúča.

```
1. # tkiptun-ng -a aa:bb:cc:dd:ee:ff -h ff:ee:dd:cc:bb:aa
mon0
```

MAC adresa karty musí byť pri tomto útoku nastavená na MAC adresu STA.

4.1.3 Wordlist Attack

Tento útok je možné realizovať len ak máme 4-way handshake, ktorý je možné získať viacerými spôsobmi, napríklad jednoduchým sniffovaním, kedy len pasívne vyčkávame na

pripojenie STA k AP. Výhodou tohto útoku je, že je v skutočnosti nedetekovatelný. V prípade, že nechceme čakať na pripojenie STA k AP, môžeme klienta, buď jedného, alebo všetkých, deautentifikovať. Klienti sa následne pokúsia o opätovné pripojenie, čím prebehne výmena úvodných správ a my získame 4-way handshake. Pre útok deautentifikácie je kriticky dôležitá sila signálu vysielaného útočníkom. Priveľmi slabý signál nemusí AP zachytiť.

Console1:

```
1. # airmon-ng start wlan0
2. # airodump-ng -c X -bssid aa:bb:cc:dd:ee:ff -w wpa mon0
```

Console2:

```
1. # aireplay-ng -1 0 -a aa:bb:cc:dd:ee:ff -c
ff:ee:dd:cc:bb:aa mon0
```

Zachytenie handshake sa zobrazí v prvej konzole v pravom hornom rohu. Jeho existenciu môžeme prípadne overiť pomocou nástroja Wireshark s filtrom „eapol“, kedy sa nám zobrazia 4 správy pre každého klienta, z ktorých sa skladá 4-way handshake. Takto odchytený Handshake sa pokúsime prelomiť niekoľkými nástrojmi.

Aircrack-ng je vďaka svojím širokým možnostiam populárny nástroj pre audit WEP/WPA-PSK/WPA2-PSK zabezpečených sietí. Obsahuje implementáciu SSE2 inštrukcií vďaka čomu je výrazne urýchlená doba hľadania kľúča [21].

```
1. # Aircrack-ng wpa-01.cap -e NazovSSID -a 2 -w dict
```

CoWPAtty je navrhnutý ako nástroj pre audit WPA-PSK založených na TKIP protokole. Od verzie 4.0 je však upravený pre podporu WPA2 s AES-CCMP [22].

```
1. # ./cowpatty -r  wpa-01.cap -f dict -s NazovSSID
```

Pyrit je nástroj na vytváranie masívnych vopred vypočítaných databáz a priameho výpočtu kľúča z odchyteného 4-way handshake za pomoci viac-jadrových procesorov a GPGPU NVIDIA CUDA a OpenCL. V súčastnosti ide o najúčinnejší útok na WPA/WPA2 PSK [23].

4.2 Prístupový bod ERS

AP sa nachádza v uzamknutej časti budovy. Fyzický prístup nieje možný. SSID identifikátor je krátky a nie je možné ho považovať za dostatočne náhodný a bezpečný.

Približne hodinovým skenovaním sa nepodarilo zistiť pripojenie žiadneho klienta k AP. Preto boli vykonané útoky na PRGA:

```
Fragmentation attack:    neúspešný      30min.
Chopchop attack:         úspešný        17min.
P0841 attack:            úspešný        22min.
```

Prístupový bod bol prelomený v priebehu pár minút pre nedostatočné zabezpečenie. Po prelomení sme nezískali žiadny prístup do firemnej siete. Pravdepodobným vysvetlením môže byť odpojenie AP od firemnej siete.

4.3 Prístupový bod ERS office service

AP sa nachádza voľne prístupné, položené v kancelárií na zemi, hrozí riziko fyzického prístupu k AP, jeho vypnutie, reset prípadne rekonfigurácia. SSID je dostatočne náhodné a môžeme ho považovať za bezpečné.

Približne 2 minúty skenovania potvrdilo nastavenie AP WPA-PSK-TKIP, kanál 2 (2417 MHz) počet pripojených klientov: 3

DoS Attack	úspešný	------
Beck Tews Attack (MIC)	úspešný	28min.
Wordlist Attack	úspešný	5hod.
Fake AP Attack	úspešný	------

4.4 Prístupový bod ERS Systems

AP sa nachádza voľne prístupné, avšak zavesené na stene vo výške približne 2m., hrozí čiastočné riziko fyzického prístupu k AP, jeho vypnutie, reset prípadne rekonfigurácia. Názov SSID môžeme považovať za dostatočne náhodný.

Približne 2 minúty skenovania potvrdilo nastavenie AP WPA-PSK-CCMP, kanál 11 (2462 MHz) pripojených klientov: 2

DoS Attack	úspešný	------
Wordlist Attack	neúspešný	24h.
Fake AP Attack	úspešný	------

Realizovaný útok na AP zameraný na získanie tajného hesla nebol úspešný.

4.5 Prístupový bod ERS Holding

AP sa nachádza v špeciálnej miestnosti s obmedzenými právami prístupu. Názov SSID je dostatočne náhodný a môžeme ho považovať za bezpečný.

Približne 2 minúty skenovania potvrdilo nastavenie AP WPA-PSK-CCMP, kanál 6 (2437 MHz) pripojených klientov: 1

DoS Attack	úspešný	------
Wordlist Attack	neúspešný	24h.
WPS Attack	úspešný	13h.
Fake AP Attack	úspešný	------

Prístupový bod bol prelomený za 13 hodín a podarilo sa nám získať tajné heslo. Dôvodom bola zapnutá funkcia WPS, viď kapitola 2.12 WPS, ktorá nie je považovaná za bezpečnú. Pôvodný útok by mal byť realizovateľný za približne 7 hodín. Dôvodom dlhšieho času útoku je pravdepodobná aplikácia obmedzení výrobcom HW ktorý útok spomalil. Po prelomení sme získali plný prístup do firemnej siete.

5 Implementácia úprav zabezpečenia a prístupových mechanizmov.

Zabrániť fyzickému prístupu je kriticky dôležitá súčasť zabezpečenia a netreba ju podceňovať. Po dlhom zvažovaní sa podarilo nájsť pre všetky AP umiestnenia, ktoré buď úplne alebo aspoň čiastočne zamedzovali priamemu prístupu k AP.

Autentizácia pomocou protokolu riadenia prístupu k sieti 802.1x bola nastavená pre jednoduchšiu správu a manažment kont prihlasujúcich sa používateľov. Pre tieto účely bol využitý centrálny server spoločnosti a ako autentizačný protokol bol zvolený PEAP-MSCHAPv2 z dôvodu zachovania čo najširšej kompatibility s používanými zariadeniami. Z dôvodu nasadenia 802.1x bolo nutné vykonať výmenu jedného zariadenia, ktoré nepodporovalo autentizáciu protokolom 802.1x a na jeden AP bol nainštalovaný alternatívny firmvér DD-WRT, ktorý nahradil pôvodný, nie veľmi stabilný firmvér.

Šifrovanie bolo na všetkých AP nastavené na WPA2 s AES-CCMP a boli aplikované pravidlá na dĺžku, formát a pravidelnú zmenu hesla. Používatelia boli riadne preškolení ohľadom bezpečnosti hesiel a používania bezdrôtových sietí. Boli spísané pravidlá, ktoré budú zapracované do smerníc informačnej bezpečnosti spoločnosti.

Názvy prístupových bodov boli zjednotené na jeden názov, ktorý používa celá budova a tým je možné prechádzať po celej budove so zariadením bez straty signálu, čo umožnila aj optimalizácia umiestnenia prístupových bodov.

5.1 Navrhované doplnkové nekomerčné riešenie

Po obvode budovy bolo navrhnuté použiť rušičky signálu, ktoré pozostávajú celkovo z 10 AP so smerovými anténami bez napojenia na vnútornú sieť. Ide o veľmi jednoduché a lacné riešenie, avšak podstatne náročnejšie na konfiguráciu či už smeru antén alebo samotnej pozície AP. Jedná sa však o cenovo najvýhodnejšie riešenie, ktoré dokáže zastaviť pokus o útok na diaľku. Pre pokus o prienik do siete musí útočník vstúpiť do budovy, kde hrozí zvýšene riziko jeho odhalenia.

Ako druhý krok bola navrhnutá implementácia začínajúceho projektu známeho pod názvom OpenWIPS-ng, ktorý v momentálnej verzii síce nedosahuje kvality porovnateľné s komerčnými riešeniami, avšak dokáže detegovať útoky na bezdrôtovú sieť a notifikovať správcu, ktorý môže podniknúť potrebné kroky. Projekt OpenWIPS by v nasledujúcich verziách podľa plánu vývoja mohla byť v budúcnosti zaujímavá nekomerčná voľba [24].

5.2 Navrhované doplnkové komerčné riešenie

Komerčných spoločnostií venujúcich sa systémom na zabezpečovanie firemných bezdrôtových sietí je niekoľko a každá z nich ponúka svoje vlastné originálne riešenie. Medzi najznámejšie patrí Aruba Networks, Airmagnet a Airtight Networks. Zo spomínaných riešení som vybral riešenie od spoločnosti Airtight networks z dôvodu jednoduchého nasadenia. Riešenie je označované ako WIPS. Ide o Cloudom riadené rádio, ktoré je možné nakonfigurovať ako AP, alebo senzor ktorý vykonáva nepretržitú kontrolu okolia a bezdrôtovej prevádzky. Zariadenie dokáže lokalizovať ako útočníka, tak aj všetkých klientov, oboznámiť správcu s problémom, či eliminovať momentálne všetky známe útoky podľa nakonfigurovanej politiky.

Na trianguláciu pozície nie sú potrebné 3 zariadenia, ale iba jedno, ktoré potrebuje minimálne práve 2 AP na zameranie pozície. Triangulácia podľa výrobcu je udávaná s presnosťou na 2-5m.

Týmto spôsobom je možné centrálne zabezpečiť a spravovať všetky oddelené pracoviská aj mimo budovy.

Jedná sa o veľmi vhodné riešenie pre zabezpečenie vysoko citlivého bezdrôtového prenosu, kde je kladený dôraz na čo najvyššie zabezpečenie. Toto riešenie je dokonca vhodné aj pre použitie na miestach, kde bezdrôtové siete nie sú vôbec povolené. V takomto prípade je možné zariadenie nastaviť spôsobom, že po zdetegovaní akejkoľvek siete ruší všetky bezdrôtové pripojenia [25].

Nevýhodou tohto riešenia je jeho obstarávacia cena a taktiež predpoklad, že žiadne zariadenie ani mechanizmus nezabráni pasívnemu útoku.

6 Záver

Bezpečnosť bezdrôtovej siete je samostatná, veľmi citlivá oblasť informačnej bezpečnosti každej spoločnosti. Vynucovať zákaz používania bezdrôtových sietí sa síce spočiatku môže javiť ako dobrý nápad, no bez monitorovania toho, čo sa deje „vo vzduchu“, nie je možné sa na takýto formálny zákaz spoliehať. Súčasný enormný nárast používania bezdrôtových zariadení ako „smartfóny“, „tablety“, či „notebooky“ vo firemnej sfére však naznačujú, že nie je možné používanie bezdrôtových prístupových bodov celkom vylúčiť a v niektorých spoločnostiach môže byť výskyt bezdrôtových AP kritický. V prípade spoločností je v takomto prípade ideálne použitie zabezpečenia typu EAP, ideálne EAP-TLS ktoré sa javí ako najbezpečnejšie, avšak nemusí byť podporované všetkými platformami, nakoľko zariadenia pre získanie certifikácie WPA2 od Wi-Fi aliancie musí spĺňať podporu protokolu PEAP, nie však plne bezpečného protokolu EAP-TLS.

Zabezpečenie bezdrôtovej siete je možné kombinovať so zariadeniami typu WIPS (Wireless Intrusion and Prevention System). WIPS je možné prirovnať k automatizovanému penetračnému pracovníkovi, ktorý neustále monitoruje bezdrôtovú sieť a na podozrivé či neadekvátne prejavy správania sa v sieti je schopný reagovať okamžite podľa vopred definovaných pravidiel. Implementáciu týchto zariadení po osobných testoch vysoko odporúčam všade tam, kde je nasadenie bezdrôtových AP nevyhnutné a cena informácií prenášaná týmto spôsobom vysoká.

Použitá literatúra

[1] GAST, Matthew. *802.11 wireless networks: the definitive guide,* 2nd ed. Sebastopol : O'Reilly, 2005. 630 s. ISBN 0-596-10052-3.

[2] Wifi [online]. 2010 [cit. 2013-12-19]. Dostupné z WWW: http://clanky.katalogmobilu.cz/slovnik-pojmu-mobilni-telefony/1430-wifi/.

[3] BRISBIN, Shelly. Wi-fi: *Postavte si svou vlastní wi-fi síť.* 2Nd ed. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.

[4] 802.11ac (Wave-1): MORE Network Engineering Insights [cit. 2013-12-25]. Dostupné z WWW: http://blog.airtightnetworks.com/802-11ac-wave-1-more-network-engineering-insights/.

[5] KOCUR, Zbyněk. – ŠAFRÁNEK, Miroslav. Fyzická vrstva Wi-Fi [online]. Praha : ČVUT, 2009. [cit. 2014-1-9]. Dostupné z WWW: http://pandatron.cz/?699&fyzicka_vrstva_wi-fi/

[6] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* 1. vyd.Brno: CP Books, 2005. 179 s. ISBN 80-251-0791-4.

[7] BARKEN, Lee. *Wi-Fi: Jak zabezpečit bezdratovou síť.* 1. vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

[8] ŠUSTR, Matej. Bezpečnost a Hacking WiFi (802.11) - 3. WEP [online]. 2007. [cit. 2014-1-9]. Dostupné z WWW: http://www.security-portal.cz/clanky/bezpečnost-hacking-wifi-80211-3-wep/

[9] AHARONI, Mati a Thomas D'OTREPPE DE BOUVETTE. OFFENSIVE SECURITY LLC. BackTrack WiFu: An Introduction to Practical Wireless Attacks. 2.0. 2009. Dostupné z: http://www.offensive-security.com/information-security-training-offensive-security-wireless-attacks/

[10] PHIFER, Lisa. The Caffe Latte Attack: How It Works -- and How to Block It. [online]. 2007 [cit. 2014-01-14]. Dostupné z: http://www.wi-fiplanet.com/tutorials/article.php/3716241

[11] MOSKOWITZ, Robert. Weakness in Passphrase Choice in WPA Interface. In: [online]. [cit. 2014-01-15]. Dostupné z: http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

[12] KWAN, Philip, WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP), [online]. URL: http://www.amsoftwareservices.net/KnowledgeBase/802_1x%20Authentication%20(AEGIS)/EAPWhitePaper.pdf

[13] ŠUSTR, Matej. *Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2.* [online]. 2007 [cit. 2013–12-27]. Dostupné z WWW: http://www.security-portal.cz/clanky/bezpečnost-hacking-wifi-80211-4-část-wpa-wpa2

[14] HILL, Joshua. An Analysis of the RADIUS Authentication Protocol In: [online]. 2001 [cit. 2014-2-11]. Dostupné z: http://www.untruth.org/~josh/security/radius/radius-auth.html

[15] BECK, Martin a Erik TEWS. Practical Attacks Against WEP and WPA. In: [online]. [cit. 2014-2-14]. Dostupné z: http://www.cs.rit.edu/~adb3160/crypto2/files/p79-tews.pdf

[16] OHIGASHI, Toshihiro a Masakatu MORII. A Practical Message Falsification Attack on WPA. In: [online]. [cit. 2014-2-18]. Dostupné z: http://hirte.aircrack-ng.org/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

[17] AIRTIGHT NETWORKS. WPA2 Hole196 Vulnerability: Exploits and Remediation Strategies: A Whitepaper by AirTight Networks, Inc. In: [online]. [cit. 2014-2-18]. Dostupné z: http://www.airtightnetworks.com/fileadmin/pdf/whitepaper/WPA2-Hole196-Vulnerability.pdf

[18] VIEHBÖCK, Stefan. Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation. In: [online]. 3. vyd. 2011 [cit. 2014-2-21]. Dostupné z: http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[19] Church of Wifi WPA-PSK Lookup Tables. In: [online]. [cit. 2014-2-19]. Dostupné z: http://www.renderlab.net/projects/WPA-tables/

[20] M1CK3Y. Giga Wordlist Creator: automatic wordlist merging & optimization for wpa cracking. In: [online]. 2010 [cit. 2014-2-21]. Dostupné z: http://www.backtrack-linux.org/forums/showthread.php?t=13882

[21] Aircrack-ng. D'OTREPPE, Thomas. *Aircrack-ng* [online]. [cit. 2013-03-02]. Dostupné z: http://www.aircrack-ng.org

[22] CoWPAtty MAIN. *CoWPAtty* [online]. [cit. 2013-03-04]. Dostupné z: http://wirelessdefence.org/Contents/coWPAttyMain.htm

[23] Pyrit. *Pyrit* [online]. [cit. 2013-03-11]. Dostupné z: http://pyrit.wordpress.com

[24] OpenWIPS-ng. D'OTREPPE, Thomas. *OpenWIPS-ng* [online]. [cit. 2013-03-15]. Dostupné z: http://openwips-ng.org

[25] AirTight NETWORKS: *Secure Cloud-Managed Wi-Fi*. AirTight NETWORKS [online]. [cit. 2013-03-18]. Dostupné z: http://www.airtightnetworks.com

[26] DRAVET, J. *Cracking Passwords Version 1.1*. [online]. 2010 [cit. 2014-04-09]. Dostupné z: http://tools.question-defense.com/Cracking_Passwords_Guide.pdf

[27] RAMACHANDRAN, Vivek. *BackTrack 5 wireless penetration testing: beginner's guide : master bleeding edge wireless testing techniques with BackTrack 5*. Birmingham [U.K.]: Packt Pub. Ltd., 2011, iv, 207 p. ISBN 978-1849515580.

[28] THOUGHTCRIME LABS. *CloudCracker: Online Hash Cracker* [online]. 2012 [cit. 2014-07-21]. Dostupné z: https://www.cloudcracker.com